

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN**

*In re StockX Customer
Data security Breach
Litigation*

Case No. 2:19-cv-12441-VAR-EAS

Honorable Victoria A. Roberts

Magistrate Judge Elizabeth A. Stafford

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs I.C., a minor by and through his natural parent, Nasim Chaudhri, M.S., a minor by and through his natural parent Shuli Shakarchi, Adam Foote, Anthony Giampetro, Kwadwo Kissi, Richard Harrington, Johnny Sacasas, and Chad Bolling, individually and on behalf of a Class defined below of similarly situated persons, allege the following against Defendants StockX, Inc., and StockX, LLC (collectively “StockX”) based upon personal knowledge and on information and belief derived from, among other things, StockX’s August 8, 2019 “Notice of Data Breach,” investigation of counsel, and review of public documents as to all other matters.

NATURE OF COMPLAINT

1. Plaintiffs bring this action against StockX for StockX’s failure to reasonably safeguard Plaintiffs’ Personally Identifiable Information (“PII”) as

defined herein, failure to reasonably provide timely notification that Plaintiffs' PII had been accessed and acquired by an unauthorized third party, and for intentionally and unconscionably deceiving Plaintiffs relating to the status, safety, location, access, and protection of Plaintiffs' PII.

2. As a result of StockX's negligent, reckless, intentional, or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiffs' PII was accessed, acquired, stolen, and re-sold by thieves for the express purpose of misusing Plaintiffs' data and causing further irreparable harm to Plaintiffs' personal, financial, reputational, and future well-being (the "Data Breach" or "Breach"). After the theft of Plaintiffs' PII from StockX's platform, it was distributed to and among hacker forums and other identity and financial thieves for the purpose of illegally misusing, reselling, and stealing Plaintiffs' PII and identity. Plaintiffs have been injured and sustained damages as a result.

3. Plaintiffs bring this lawsuit against StockX for statutory violations as well as common law tort claims of negligence, negligent misrepresentation, fraud and silent fraud, negligence per se, unjust enrichment, violation of state Data Breach statutes, violation of state consumer protection laws, intrusion upon seclusion, bailment, and declaratory judgment.

4. As used throughout this Complaint, “Personally Identifiable Information” or “PII” is defined as all information exposed by the StockX Data Breach, includes all information so defined under individual states’ statutes and includes, but is not limited to, any combination of name, address, birth date, Social Security number, driver’s license information (any part of license number, state, home address, dates of issuance or expiration), telephone number, email address, tax identification number, credit card number, usernames, passwords, and log-in information that can be used to access a person’s personal electronic content.

PARTIES

Plaintiff I.C.

5. Plaintiff I.C., a minor, brings this suit by and through his natural parent, Nasim Chaudhri. Plaintiff I.C. and Nasim Chaudhri are individual citizens and residents of Kansas. Minor Plaintiff had a StockX account at the time of the incidents described herein and entrusted PII to StockX with the reasonable expectation and understanding that StockX would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiffs’ PII.

6. Like all other members of the Class, Plaintiff provided his first name, last name, username, email address, password, shoe size, and/or other information, to StockX.

7. Plaintiff did not learn of the StockX Breach until StockX informed him of the same via email on August 8, 2019—thirteen (13) days after StockX claims to have learned of the breach, seven (7) days after StockX requested that he and the Class reset their passwords due to purported “system updates,” five (5) days after StockX sent a generic “data security update,” and approximately three (3) months after the Breach took place.

8. Plaintiff would not have created an account with and provided his sensitive and valuable PII to StockX had StockX disclosed that it lacked computer systems and data security practices sufficient to adequately safeguard his and other consumers’ PII or that StockX would not be completely forthright or honest with Plaintiff in the event of a Data Breach.

9. Plaintiff has been injured and sustained damages as a result of the Data Breach and the disclosure of his PII. Further, he will continue to expend, time, money, and/or resources to manage the ongoing threat and future consequences resulting from the Data Breach; and he suffers from a present, immediate and

imminent and continuing risk of harm, including but not limited to, the serious and immediate risk of fraud and identity theft.

10. Plaintiff has refrained from using StockX since he became aware of the Data Breach.

Plaintiff Adam Foote

11. Plaintiff Adam Foote is an individual citizen and resident of Kansas who had a StockX account at the time of the incidents described herein and entrusted his PII to StockX with the reasonable expectation and understanding that StockX would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiffs' PII.

12. Like all other members of the Class, Plaintiff provided his first name, last name, username, email address, password, shoe size, and/or other information, including payment and banking information, to StockX.

13. Plaintiff did not learn of the StockX Breach until StockX informed him of the same via email on August 8, 2019—thirteen (13) days after StockX claims to have learned of the breach, seven (7) days after StockX requested that he and the Class reset their passwords due to purported “system updates,” five (5) days after StockX sent a generic “data security update,” and approximately three (3) months

after the Breach took place.

14. The Breach already has required Plaintiff to expend significant time and energy to protect himself from the Breach's potential adverse consequences, including but not limited to investigating whether hackers have further attempted to misuse his PII, and potential means by which to protect himself from identity theft, such as updating other online accounts, including but not limited to, those for which he used the same email address and/or password as his StockX account, and monitoring associated bank and credit accounts.

15. Subsequent to the Data Breach, Plaintiff has experienced no less than 14 instances of identity theft and/or illegitimate activity on various accounts, including his Sony, Nintendo, Netflix ,and Hulu accounts, beginning in approximately August 2019 and occurring up through and including March 2020. Mr. Foote has expended extensive time and effort monitoring, updating, and resolving issues relating to his online accounts following the StockX Data Breach.

16. Through investigation and upon information and belief, Plaintiff did not experience any instances of identity theft and/or illegitimate activity on the aforementioned accounts prior to the StockX Data Breach.

17. Plaintiff would not have created an account with and provided his sensitive and valuable PII to StockX had StockX disclosed that it lacked computer

systems and data security practices sufficient to adequately safeguard his and other consumers' PII or that StockX would not be completely forthright or honest with Plaintiff in the event of a Data Breach.

18. Plaintiff has been injured and sustained damages as a result of the Data Breach and the disclosure of his PII. Further, he will continue to expend, time, money, and/or resources to manage the ongoing threat and future consequences resulting from the Data Breach; and he suffers from a present, immediate and imminent and continuing risk of harm, including but not limited to, the serious and immediate risk of fraud and identity theft

Plaintiff M.S.

19. Plaintiff M.S., a minor by and through his natural parent and legal guardian, Shuli Shakarchi, had a StockX account at the time of the incidents described herein and entrusted his PII to StockX with the reasonable expectation and understanding that StockX would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiffs' PII. Plaintiff M.S. and Shuli Shakarchi are individual citizens and residents of New Jersey.

20. Plaintiff created a StockX account on February 25, 2018. Like all other members of the Class, Plaintiff provided his first name, last name, username, email address, password, shoe size, and/or other information.

21. Plaintiff did not learn of the StockX Breach until StockX informed him of the same via email on August 8, 2019—thirteen (13) days after StockX claims to have learned of the breach, seven (7) days after StockX requested that he and the Class reset their passwords due to purported “system updates,” five (5) days after StockX sent a generic “data security update,” and approximately three (3) months after the Breach took place.

22. Plaintiff would not have created an account with and provided his sensitive and valuable PII to StockX had StockX disclosed that it lacked computer systems and data security practices sufficient to adequately safeguard his and other consumers’ PII or that StockX would not be completely forthright or honest with Plaintiff in the event of a Data Breach.

23. Plaintiff has been injured and sustained damages as a result of the Data Breach and the disclosure of his PII. Further, he will continue to expend, time, money, and/or resources to manage the ongoing threat and future consequences resulting from the Data Breach; and he suffers from a present, immediate and

imminent and continuing risk of harm, including but not limited to, the serious and immediate risk of fraud and identity theft.

Plaintiff Chad Bolling

24. Plaintiff Chad Bolling is an individual citizen and resident of the State of California who had a StockX account at the time of the incidents described herein and entrusted PII (as defined herein) to StockX with the reasonable expectation and understanding that StockX would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiff Bolling's PII. Plaintiff Bolling has bought and sold goods on the StockX platform.

25. Plaintiff Bolling created a StockX account in or around 2016. Like all other members of the Class, Plaintiff provided his first name, last name, username, email address, password, shoe size, and/or other information to StockX.

26. Plaintiff did not learn of the StockX Breach until StockX informed him of the same via email on August 8, 2019—thirteen (13) days after StockX claims to have learned of the breach, seven (7) days after StockX requested that he and the Class reset their passwords due to purported “system updates,” five (5) days after StockX sent a generic “data security update,” and approximately three (3) months after the Breach took place.

27. The Breach already has required Plaintiff to expend significant time and energy to protect himself from the Breach's potential adverse consequences, including but not limited to investigating whether hackers have further attempted to misuse his PII, and potential means by which to protect himself from identity theft, such as updating other online accounts, including but not limited to, those for which he used the same email address and/or password as his StockX account, and monitoring associated bank and credit accounts.

28. Since the Data Breach, Mr. Bolling has received notices of unauthorized access to numerous accounts that shared the same credentials as were compromised in the Data Breach. These include accounts associated with the online game platform STEAM. He also received notification of either unauthorized access, unusual activity, or unauthorized access attempts at the following websites: Reddit, Caviar (a food delivery service), Spotify, and Footlocker. The Reddit and Spotify account compromises were particularly disturbing to Mr. Bolling as these could reveal personal correspondence that was intended to be anonymous, as well as his personal music listening history, in addition to other PII that may have been stored in these locations which was now exposed to unauthorized third parties.

29. After receiving the notice of unauthorized activity as to his Reddit account in December 2019, Mr. Bolling began the process of changing the username

and/or password on his numerous online accounts. Following the notice of unauthorized access to his Spotify account in February 2019, Mr. Bolling spent an entire day changing usernames and/or passwords for all of his accounts that he could identify. Mr. Bolling estimates that, all told, he spent between 20 and 40 hours identifying online accounts that may have been affiliated with his credentials that were stolen in the Data Breach, and then changing the username and/or password for each of those online accounts.

30. Plaintiff Bolling would not have created an account with and provided his sensitive and valuable PII to StockX had StockX disclosed that it lacked computer systems and data security practices sufficient to adequately safeguard his and other consumers' PII or that StockX would not be completely forthright or honest with Plaintiff in the event of a Data Breach..

31. Plaintiff has been injured and sustained damages as a result of the Data Breach and the disclosure of his PII. Further, he will continue to expend, time, money, and/or resources to manage the ongoing threat and future consequences resulting from the Data Breach; and he suffers from a present, immediate and imminent and continuing risk of harm, including but not limited to, the serious and immediate risk of fraud and identity theft.

Plaintiff Johnny Sacasas

32. Plaintiff Johnny Sacasas is a citizen and resident of the State of Florida who had a StockX account at the time of the incidents described herein and entrusted PII to StockX with the reasonable expectation and understanding that StockX would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiff Sacasas' PII.

33. Plaintiff Sacasas created a StockX account in 2017 or 2018. Like all other members of the Class, Plaintiff provided his first name, last name, username, email address, password, shoe size, and/or other information, including payment and banking information, to StockX.

34. Plaintiff Sacasas has both bought and sold goods on the StockX platform.

35. Plaintiff did not learn of the StockX Breach until StockX informed him of the same via email on August 8, 2019—thirteen (13) days after StockX claims to have learned of the breach, seven (7) days after StockX requested that he and the Class reset their passwords due to purported “system updates,” five (5) days after StockX sent a generic “data security update,” and approximately three (3) months after the Breach took place.

36. The Breach already has required Plaintiff to expend significant time and

energy to protect himself from the Breach's potential adverse consequences, including but not limited to investigating whether hackers have further attempted to misuse his PII, and potential means by which to protect himself from identity theft, such as updating other online accounts, including but not limited to, those for which he used the same email address and/or password as his StockX account, and monitoring associated bank and credit accounts.

37. After receiving notice of the Data Breach, Mr. Sacasas attempted to remove his credit card information from his StockX account. However, the StockX platform would not allow him to do so unless he replaced the existing information with new payment card information. Thus, Mr. Sacasas was left with no choice but to leave his financial information stored on the StockX platform.

38. Then, or about March 11, 2020, an unauthorized third party accessed Mr. Sacasas' StockX account and changed the physical address and phone number associated with the account. The unauthorized third party attempted to make two large purchases: a Louis Vuitton belt for \$617.26 and a pair of Jordan 1 Retro High Fearless UNC Chicago sneakers for \$287.80. Fortunately, these transactions were flagged as fraudulent and Mr. Sacasas received notification.

39. Mr. Sacasas had to address the hack of his StockX account when he first received the notification of the attempted fraudulent transaction on or about March

11, 2020 and again the following day when he had to take additional steps to secure his account at the direction of StockX. This required him to step away from his work. Mr. Sacasas estimates spending 15-30 minutes securing his account.

40. In addition to securing his StockX account, because he was concerned that his financial information may have been exposed to the third party who accessed his account, Mr. Sacasas reviewed his credit card and debit card account statements shortly after the fraudulent purchase attempts on or about March 11, 2020.

41. Mr. Sacasas estimates spending about 15-20 minutes reviewing these statements. Mr. Sacasas continues to monitor his credit and debit card account statements, as well as his PayPal account (which was also linked to his StockX account) to guard against further ramifications from the Data Breach and the attendant hack on his StockX account. He estimates spending about 15-20 minutes each month reviewing these accounts.

42. Plaintiff Sacasas would not have created an account with and provided his sensitive and valuable PII to StockX had StockX disclosed that it lacked computer systems and data security practices sufficient to adequately safeguard his and other consumers' PII or that StockX would not be completely forthright or honest with Plaintiff in the event of a Data Breach.

43. Plaintiff has been injured and sustained damages as a result of the Data Breach and the disclosure of his PII. Further, he will continue to expend, time, money, and/or resources to manage the ongoing threat and future consequences resulting from the Data Breach; and he suffers from a present, immediate and imminent and continuing risk of harm, including but not limited to, the serious and immediate risk of fraud and identity theft.

Plaintiff Anthony Giampetro

44. Plaintiff Anthony Giampetro is a citizen and resident of the State of New York who had a StockX account at the time of the incidents described herein and entrusted PII to StockX with the reasonable expectation and understanding that StockX would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiff Giampetro's PII. Plaintiff Giampetro has both bought and sold goods on the StockX platform.

45. Like all other members of the Class, Plaintiff provided his first name, last name, username, email address, password, shoe size, and/or other information, including payment and banking information, to StockX.

46. Plaintiff did not learn of the StockX Breach until StockX informed him of the same via email on August 8, 2019—thirteen (13) days after StockX claims to

have learned of the breach, seven (7) days after StockX requested that he and the Class reset their passwords due to purported “system updates,” five (5) days after StockX sent a generic “data security update,” and approximately three (3) months after the Breach took place.

47. What’s more, Plaintiff Giampetro believes hackers used his account to make five (5) attempted fraudulent purchases without his knowledge or consent. Plaintiff Giampetro further believes that one of the attempted fraudulent purchases was successful but StockX still refused to reimburse him for the fraudulent purchase.

48. As a result of the Data Breach, Plaintiff has expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the future consequences of the Data Breach including investigating the information compromised and how best to ensure he is protected from potential identity theft and fraud, which efforts are continuous and ongoing.

49. Plaintiff would not have created an account with and provided his sensitive and valuable PII to StockX had StockX disclosed that it lacked computer systems and data security practices sufficient to adequately safeguard his and other consumers’ PII.

50. Plaintiff has been injured and sustained damages as a result of the Data Breach and the disclosure of his PII. Further, he will continue to expend, time,

money, and/or resources to manage the ongoing threat and future consequences resulting from the Data Breach; and he suffers from a present, immediate and imminent and continuing risk of harm, including but not limited to, the serious and immediate risk of fraud and identity theft.

Plaintiff Richard Harrington

51. Plaintiff Richard Harrington is a citizen and resident of the State of New York who had a StockX account at the time of the incidents described herein and entrusted PII to StockX with the reasonable expectation and understanding that StockX would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiff Harrington's PII. Plaintiff Harrington has both bought and sold goods on the StockX platform.

52. Plaintiff Harrington created a StockX account in approximately 2018. Like all other members of the Class, Plaintiff provided his first name, last name, username, email address, password, shoe size, and/or other information, including payment and banking information, to StockX.

53. Plaintiff did not learn of the StockX Breach until StockX informed him of the same via email on August 8, 2019—thirteen (13) days after StockX claims to have learned of the breach, seven (7) days after StockX requested that he and the

Class reset their passwords due to purported “system updates,” five (5) days after StockX sent a generic “data security update,” and approximately three (3) months after the Breach took place.

54. As a result of the Data Breach, Plaintiff has expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the future consequences of the Data Breach including investigating the information compromised and how best to ensure he is protected from potential identity theft and fraud, which efforts are continuous and ongoing.

55. Plaintiff Harrington would not have created an account with and provided his sensitive and valuable PII to StockX had StockX disclosed that it lacked computer systems and data security practices sufficient to adequately safeguard his and other consumers’ PII or that StockX would not be completely forthright or honest with Plaintiff in the event of a Data Breach.

56. Plaintiff has been injured and sustained damages as a result of the Data Breach and the disclosure of his PII. Further, he will continue to expend, time, money, and/or resources to manage the ongoing threat and future consequences resulting from the Data Breach; and he suffers from a present, immediate and imminent and continuing risk of harm, including but not limited to, the serious and immediate risk of fraud and identity theft.

Kwadwo Kissi

57. Plaintiff Kwadwo Kissi is a citizen and resident of the State of Georgia who had a StockX account at the time of the incidents described herein and entrusted PII to StockX with the reasonable expectation and understanding that StockX would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiff Kissi's PII. Plaintiff Kissi has both bought and sold goods on the StockX platform.

58. Like all other members of the Class, Plaintiff provided his first name, last name, username, email address, password, shoe size, and/or other information, including payment and banking information, to StockX.

59. Plaintiff did not learn of the StockX Breach until StockX informed him of the same via email on August 8, 2019—thirteen (13) days after StockX claims to have learned of the breach, seven (7) days after StockX requested that he and the Class reset their passwords due to purported “system updates,” five (5) days after StockX sent a generic “data security update,” and approximately three (3) months after the Breach took place.

60. What's more, Plaintiff Kissi believes hackers published his personal information stolen in the Data Breach on the “dark web”.

61. Plaintiff Kissi further believes his credit rating dropped 71 points as a direct and proximate result of the injuries he sustained in the Data Breach. As a result, he had difficulty buying a home and was required to file disputes with credit bureaus.

62. As a result of the Data Breach, Plaintiff has expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the future consequences of the Data Breach including investigating the information compromised and how best to ensure he is protected from potential identity theft and fraud, which efforts are continuous and ongoing.

63. Plaintiff would not have created an account with and provided his sensitive and valuable PII to StockX had StockX disclosed that it lacked computer systems and data security practices sufficient to adequately safeguard his and other consumers' PII.

64. Plaintiff has been injured and sustained damages as a result of the Data Breach and the disclosure of his PII. Further, he will continue to expend, time, money, and/or resources to manage the ongoing threat and future consequences resulting from the Data Breach; and he suffers from a present, immediate and imminent and continuing risk of harm, including but not limited to, the serious and immediate risk of fraud and identity theft.

Defendants

63. StockX, Inc. is a Delaware corporation with its principal place of business in Detroit, Michigan.

64. StockX, LLC, is a Michigan limited liability company with its principal place of business in Detroit, Michigan.

JURISDICTION AND VENUE

65. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of \$5,000,000, the number of class members exceeds 100, and StockX is a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

66. This Court has personal jurisdiction over StockX, Inc. and StockX, LLC because they are authorized to and regularly conduct business in Michigan and are headquartered in Detroit, Michigan.

67. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in Michigan.

GENERAL ALLEGATIONS

I. *StockX – Background.*

68. StockX is an e-commerce platform for luxury goods, fashion clothing, and accessories, with a particular emphasis on ultrarare, custom, vintage, and highly sought-after shoes for “sneakerheads,” including minors.

69. Under StockX’s business model, products posted on its platform are treated similarly to the way in which stocks are traded on the market — i.e., each product is assigned a ticker symbol, sellers put out asking prices, and then prospective purchasers can bid on the products. Users of StockX then see data such as price volatility, highs, and lows from across the internet; and once a bid matches with an asking price, the sale occurs automatically.¹ StockX then takes a flat commission on each sale ranging from 8–9.5 percent.²

70. For example, in January of 2018, StockX sold limited-edition LeBron James shoes for an average of \$6,000 per pair—with approximately \$500 of each sale going directly to StockX. The shoes could then be “flipped” on the same StockX

¹ <https://www.nytimes.com/2018/07/06/business/smallbusiness/stockx-sneakerheads-luxury-goods.html?smid=nytcore-ios-share&module=inline> (Last visited, May 11, 2020) (Exhibit 1).

² *Id.*

marketplace, with StockX, again, realizing its commission, without the purchaser ever taking actual physical possession of the shoes.³

71. Some sneakers on StockX have been sold for as high as \$30,000; and at one time, the site had sneakers with an asking price of \$850,000.⁴

72. StockX has grown rapidly since its inception in February 2016. As of mid-2018, StockX was conducting more than 10,000 transactions per day, had 370 employees, and more than \$700 million in total sales.

73. More recently, StockX reported sales of \$100 million per month, and in June 2019, StockX raised \$110 million in financing (on top of a previous \$60 million), valuing it at more than \$1 billion and in excess of 800 employees.⁵

74. StockX targets minors as part of its business model.

75. One of StockX's principal targeted demographics includes pre-teen and early-teen minors.

³ *Id.*

⁴ <https://www.sportswear-international.com/news/portrait/Marketplace-How-StockX-is-revolutionizing-the-sneaker-reseller-business-online-14099> (Last visited, May 11, 2020) (Exhibit 2).

⁵ <https://www.freep.com/story/money/business/2019/06/26/stockx-valuation-ceo-scott-cutler/1569408001/> (Last visited, August 2019) (Exhibit 3).

76. It is well-known that a large segment of StockX's user base is comprised of teenagers who have not yet reached the age of majority, and StockX has profited handsomely from their use of its services.

77. The teenage demographic is a particularly active segment of StockX's user population — as teenagers are disproportionately likely to be among those highly passionate about amassing and collecting custom-made, ultrarare, vintage, and fashionable sneakers — and one of the main reasons for StockX's meteoric success.

78. On June 26, 2019, the Wall Street Journal published an article describing StockX as the “Latest \$1 Billion Unicorn” and how StockX had “closed a round of venture funding that valued the startup at more than \$1 billion” by “riding the sneaker-reselling craze fueled by teens.” And in an April 2019 article, Vox observed that “StockX has benefited from the rising popularity of acquiring tough-to-buy sneakers, especially among millennial men and teenage boys.”

79. Daniel Gilbert, co-founder of StockX, personally acknowledged the importance of the teenage market to StockX's business strategy in an interview with Sole Collector back in February 2016, shortly after StockX was formed: “The amount of interest and activity among my boys and their friends about sneakers was just

crazy,”⁶ Gilbert said. “Then I start asking other people that have teenage boys, and it’s almost 90-95 percent of the people that I asked said the same thing.” *Id.*

80. StockX has become a “leading gauge of market value in the sneaker world”⁷ and now sponsors large trade shows to which teenage, and pre-teenage, kids flock.

II. *Data breaches Pose Significant Threats to Consumers*

81. Data breaches have become a constant threat, and without adequate safeguards consumer data is vulnerable to theft from malicious actors.

82. The Identity Theft Resource Center, a non-profit established to assist victims of identity theft, cautions consumers not to discount the risks that arise from the exposure of purportedly “non-sensitive” PII: “A consumer’s identity is similar to that of a puzzle and the more accurate pieces a thief has about someone, the more they can successfully represent that person.”⁸

83. The negative repercussions of identity theft cannot be overstated: “Thieves may use your account information to make purchases online or try to empty

⁶ <https://solecollector.com/news/2016/02/campless-stockx-dan-gilbert> (last accessed May 11, 2020) (Exhibit 4)

⁷ <https://www.freep.com/story/money/business/2019/06/26/stockx-valuation-ceo-scott-cutler/1569408001/> (last accessed May 11, 2020) (Exhibit 3)

⁸ <https://www.wombatsecurity.com/blog/number-of-u.s.-data-breaches-dip-in-2018-but-pii-exposure-jumps-126> (last visited May 11, 2020) (Exhibit 5).

your bank account ... thieves can even commit identity theft and open accounts in your name. These accounts can land on your credit report, severely damaging your credit and your ability to borrow in the future. Once you've become a victim of identity theft, fighting it can be a long, complicated process.”⁹

84. By way of example, access to the same email address and/or password consumers use for a single online platform can provide unauthorized users access to consumers' other online accounts, including but not limited to, those. Once hackers have identified those additional platforms, they can attempt to access consumers' accounts and misappropriate PII stored thereon, or impersonate those platforms in order to engage in sophisticated “phishing attacks” used to trick consumers into inadvertently providing more sensitive PII or even to directly steal money.

85. The effects of the Data Breach on individuals are severe and long-lasting. Not simply a one-time occurrence, the identities of affected individuals are forever compromised. Identity thieves can use the compromised information to perpetrate a wide variety of crimes against Plaintiffs and the Class members, including those involving tax fraud; fraud pertaining to credit cards and loan accounts;

⁹ <https://www.identityiq.com/identity-theft/how-the-dark-web-can-threaten-your-credit-and-financial-security-2/> (last visited, May 11, 2020) (Exhibit 6)

fraudulent identity-related representations to the government; fraudulent medical claims; and procuring fraudulent government benefits.

86. Annual monetary losses from identity theft cost innocent individuals billions annually, and according to the United States Bureau of Justice Statistics, the losses from incidents of identity theft exceeded \$17 billion in 2016.¹⁰

87. In addition to direct financial losses, “individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.” Moreover, “in addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and pen new ones, and dispute charges with individual creditors.”¹¹

¹⁰ https://www.bjs.gov/content/pub/pdf/vit16_sum.pdf (last accessed May 11, 2020) (Exhibit 7)

¹¹ <http://www.ftc.gov/sites/default/files/documents/reports/combating-identity->

88. Stealing the identity of minors is especially attractive to cyber criminals for a host of reasons, including: (1) minors' credit reports are clean, which makes them particularly valuable; (2) minors do not check their credit reports or review monthly bills the way adults do; (3) thieves are more likely to have unfettered access to minors' identity and credit for years or even decades; (4) it is often difficult or impossible to place a freeze on a minor's credit report—because they don't yet have credit; and (5) minors are less likely to receive notice, or to have an opportunity to take notice in the event that identity theft occurs or is ongoing, such as, e.g., if fraudulent accounts or charges occur under their names, if fake tax returns are filed in their names, if fraudulent health care is obtained under their identity, and if their information is fraudulently used in connection with employment.

89. For these and other reasons, identity theft is a growing problem in the United States as it relates to our minor population. More than 1 million minors were victims of identity theft or fraud in 2017, totaling \$2.6 billion in fraudulent activity.¹²

90. In fact, in 2017, among notified breach victims, 39% of minors became victims of actual fraud (as opposed to 19% of adults).¹³

theft-strategic-plan/strategicplan.pdf, at 11 (last accessed May 11, 2020) (exhibit 8).

¹² <https://www.cnbc.com/2019/07/12/how-to-protect-your-child-from-identity-theft.html> (last visited May 11, 2020) (Exhibit 9)

¹³ <https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html> (last visited May 11, 2020) (Exhibit 10)

91. Minors are a particularly vulnerable and defenseless group of StockX users because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

92. According to a report on child identity theft published by Carnegie Mellon, a study based on identity protection scans of 40,000 U.S. children, the risk that someone was using their social security number was 51 times higher than the rate for adults in the same population, with the largest fraud being against a 16-year-old girl for \$725,000.

93. Based on StockX's laser-focus on its young teenage demographic, StockX was well aware of the economic and reputational value of exploiting that market for its own monetary gain, and it should have been equally concerned with protecting the PII entrusted to it by that valuable and relatively defenseless group.

III. *StockX Collects Personally Identifiable Information From Its Users*

94. StockX requires all individuals who wish to use its platform to create a StockX user account, which requires the prospective user to submit certain PII to StockX.

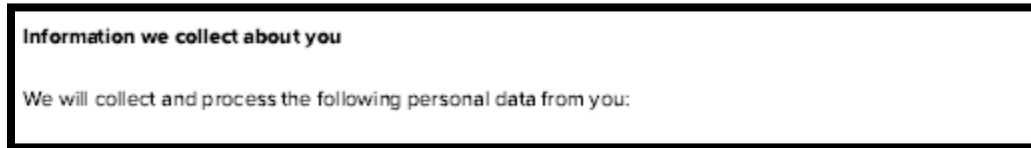
95. The information that StockX requires for prospective users to become active users initially includes the user's first name, last name, email address, a username, and a password.

96. The PII collected and retained by StockX includes, inter alia, name, address, email address and phone number, financial and credit card information, login and password details, as well as additional data StockX collects and stores, such as IP addresses, the operating system and platform used to access the site, and the products consumers search for and purchase, including shoe sizes and shopping preferences. StockX's customers, in other words, entrust StockX with their sensitive and valuable PII.

97. Plaintiffs, like all other members of the Class, created a user account on StockX's platform, and provided their first name, last name, username, email address, password, and other information to StockX.

98. StockX failed to advise its users what information it does and will collect from them, even though it requires all prospective users to provide sensitive

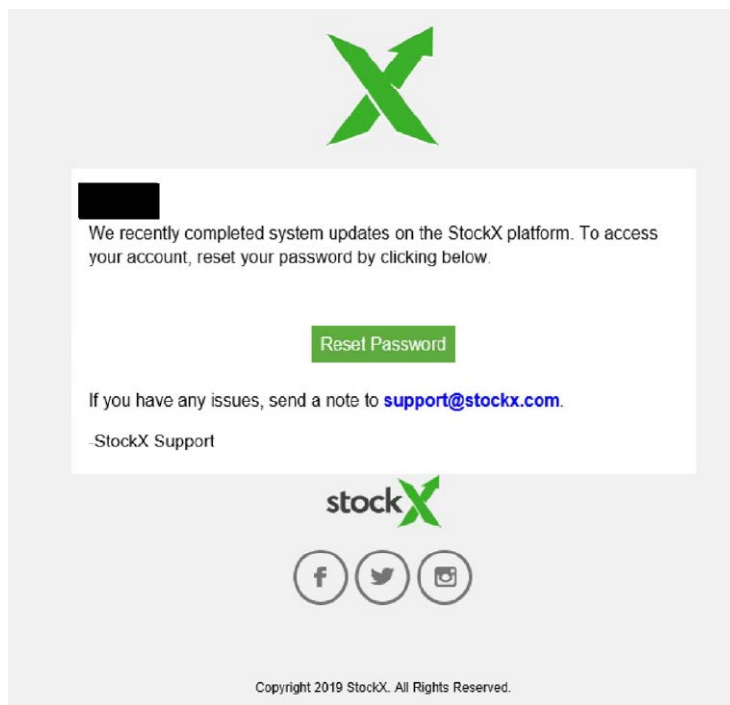
information at the very outset of their membership on the StockX platform. The first item listed in StockX's Privacy Policy purported to be information regarding "personal data" that StockX collects from its users; however, that section of the Privacy Policy was blank as shown in the below screen shot:



99. Nevertheless, StockX assures its users that it protects their information on "secure servers" and claimed that "[o]nce we have received your information, we will use strict procedures and security features to try to prevent unauthorised access." Plaintiffs and the Class Members reasonably relied on these purported security measures in deciding to provide their Personal Data to StockX.

IV. The Data Breach and StockX's Attempted Cover-up

100. On August 1, 2019, StockX sent its users, including Plaintiffs and the Class, an email notification advising that StockX had "recently completed system updates on the StockX platform" and requiring them to reset their passwords.



101. This notification was based on a deception. In reality, StockX’s password-reset notification was not a result of “system updates,” as StockX falsely claimed; rather, StockX had experienced a Data Breach several months before the notification.

102. According to several news stories published on August 3, 2019—several days after StockX’s fake “system updates” email—more than 6.8 million user accounts were stolen from StockX by a hacker in May 2019, who then listed the stolen data on the “dark web,” an encrypted online area not indexed by conventional search engines that functions, in part, as a marketplace for thieves to buy and sell stolen PII.¹⁴

¹⁴ See <https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/> (Last accessed, August 2019) (Exhibit 11).

103. Information relating to this Data Breach was provided to TechCrunch, a media outlet emphasizing technology and cyber news, by an “unnamed Data Breached seller,” who advised that the data was for sale on the dark web and provided TechCrunch with a sample of 1,000 records. Tech Crunch confirmed this information by contacting customers and providing them information from the stolen records that only the actual customers would know.¹⁵

104. Following publication of the news stories relating to the Data Breach, StockX sent a second email to its user base on August 3, 2019 with the generic subject line “Data Security Update,” acknowledging the Data Breach and admitting that the Data Breach was the real reason StockX had issued the previous password-reset email.

105. StockX further advised its users, including Plaintiffs and the Class, that, according to then-known information, an unknown third-party had been able to gain access to certain customer data, including customer name, email address, shipping address, username, password, and purchase history.

106. On August 8, 2019, StockX sent another email to its users titled “Notice of Data Breach,” stating that it was alerted to “suspicious activity potentially

¹⁵ <https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/> (Last visited, August 2019) (Exhibit 11).

involving customer data” on July 26, 2019—6 days before their false “system updates” email and 8 days before StockX apprised its users that it had been hacked. If true, given that the Data Breach occurred in May 2019, StockX was unaware for months that Plaintiffs’ and the Class Members’ PII was being compromised, further corroborating the deficiency of StockX’s security measures.

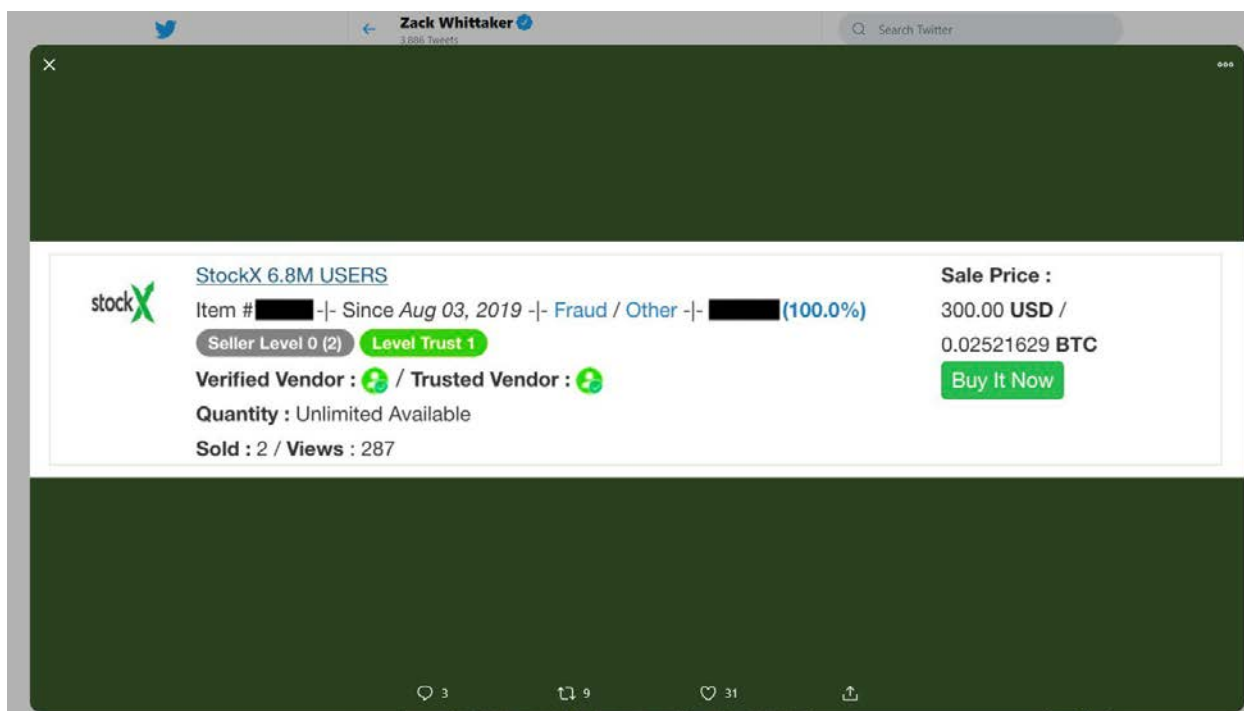
107. According to StockX’s belated notice to Plaintiffs and the Class of the Data Breach, at minimum, each Plaintiff’s “name, email address, address, username, hashed passwords, and purchase history” were disclosed in the Data Breach.¹⁶

108. The information stolen from StockX included usernames and passwords—PII that is highly valued amongst cyber thieves and criminals on the Dark Web. In fact, there is a well-established market for stolen account credentials on the Dark Web, including StockX credentials.¹⁷

109. In early reports, prior to StockX notifying Plaintiffs and the Class that their PII had been stolen, the StockX data had already been sold at least twice on the dark web:

¹⁶ StockX, Update on Data Security Issue (Aug. 8, 2019), <https://stockx.com/news/update-on-data-security-issue/> (last accessed May 5, 2020) (Exhibit 12).

¹⁷ <https://krebsonsecurity.com/2017/12/the-market-for-stolen-account-credentials/> (Last visited, August 2019) (Exhibit 13); <https://www.techradar.com/news/nearly-620-million-stolen-accounts-for-sale-on-dark-web> (Last visited, August 2019) (Exhibit 14).



110. Unsurprisingly, some users appear to have been defrauded in the time between StockX’s deceptive August 1 “system update” email and the August 3 email acknowledging that StockX had been hacked. One such user posted on Twitter posted a screenshot of an allegedly fraudulent purchase for a Jordan 1 sneaker for more than \$23,000 that occurred between the August 1 and August 3 emails from StockX.

111. On information and belief, one way in which criminals could leverage the stolen StockX data for a highly profitable enterprise. The criminals purchase the StockX data and thereby obtain Plaintiffs’ and the Class’s stolen PII, including email address, usernames, passwords, shipping addresses, etc.; StockX sends its users a password-reset email based on its fake “system update” notice; the criminals trigger

a password-reset through StockX's system and intercept the confirmation email by logging in to the user's email using the stolen StockX PII; and the criminal updates the StockX password and initiates fraudulent purchases redirecting either the funds, the merchandise, or both.






112. The PII that Plaintiffs and the Class entrusted to StockX has been stolen, sold, and purchased by criminals who will seek and have already sought to misuse it.

113. According to more recent reporting, bad actors "have already begun to decrypt the stolen passwords and it is expected for this information to be used in future attacks."¹⁸

114. The stolen information has also been added to the Data Breach monitoring website, "Have I Been Pwned,"¹⁹ which added the StockX database to their website so users can check to see if their email was included in the breach. As shown in the below screenshot from "Have I Been Pwned," 6,840,399 accounts were stolen from StockX.

¹⁸ <https://www.bleepingcomputer.com/news/security/database-from-stockx-hack-sold-online-check-if-youre-included/> (Last visited, August 2019) (Exhibit 15).

¹⁹ <https://haveibeenpwned.com/> (pronounced "poned") (Last visited, August 2019) (Front page of website attached as Exhibit 16, reference to StockX breach on PDF page 2).

Recently added breaches		
	749,161	<u>Cracked.to accounts</u>
	6,840,339	<u>StockX accounts</u>
	137,272,116	<u>Canva accounts</u>
	23,205,290	<u>CafePress accounts</u>
	4,007,909	Club Penguin Rewritten (July

115. A search of “Have I Been Pwned” confirms that Plaintiffs’ information was exposed as a result of the StockX Data Breach.²⁰

116. The Data Breach is truly massive in scope, affecting nearly 7 million accounts. The repercussions are still being felt at the present and could last for the lifetime of the individuals. The compromised information allows criminals to potentially access every aspect of an individual’s digital footprint.

117. The username and password combinations are now being distributed on underground hacker forums for a de minimus amount, which virtually guarantees they it will be widely distributed. And for those cybercriminals who do not want to go through the trouble of decrypting the user accounts, they can purchase up to 367,000 decrypted accounts (of the more than 6.8 million stolen accounts) for \$400.²¹

²⁰ <https://www.bleepingcomputer.com/news/security/database-from-stockx-hack-sold-online-check-if-youre-included/> (Last visited, August 2019) (Exhibit 15).

²¹ *Id.*

118. Now that the stolen data is widely available for a minimal sum, the credentials will be used in “credential stuffing” attacks, which involve thieves compiling and using usernames and passwords that were leaked from different Data Breaches to try and gain access to accounts at other sites.²²

119. The founder of Rendition Infosec, a cybersecurity firm staffed by former National Security Agency, Department of Defense, and US Cyber Command Operators, stated that StockX’s misleading conduct “robbed their users of the chance to evaluate their exposure” by not informing its users of the breach when it happened.²³

120. Plaintiffs’ and the Class Members’ PII was among the confidential information compromised in the StockX Data Breach, causing Plaintiffs and the Class to suffer injury and damages, including but not limited to the improper disclosure of the PII, the loss of the value of the PII, ongoing disclosures and dissemination of the PII, the imminent and ongoing threat of identity theft and other fraud against Plaintiffs and the Class, the loss of Plaintiffs’ and the Class’s privacy, and out-of-pocket

²² <https://www.wired.com/story/what-is-credential-stuffing/> (Last visited, August 2019) (Exhibit 14); <https://www.bleepingcomputer.com/news/security/database-from-stockx-hack-sold-online-check-if-youre-included/> (Last visited, August 2019) (Exhibit 17).

²³ <https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/> (Last visited, August 2019) (Exhibit 11).

expenses and time devoted to mitigating the effects of the Data Breach and ascertaining the extent of Plaintiffs' and the Class's losses and exposure.

121. Plaintiffs and the Class would never have provided their PII to StockX if it was known the security provided by StockX was not reasonable security or that StockX was not providing the security that StockX represented it would provide, as was revealed by the Data Breach described by media outlets following StockX's false "system updates" email.

122. Plaintiffs and the Class would further never have provided their PII to StockX if they had known that StockX would seek to deceive Plaintiffs and the Class in the event that StockX was subject to a Data Breach or that StockX would not be completely forthright or honest with Plaintiffs and the Class in the event of a Data Breach.

123. Plaintiffs and the Class would never have provided their PII to StockX if StockX had disclosed that it lacked adequate security measures and data security practices.

124. Plaintiffs and the Class have been injured and damaged in that Plaintiffs and the Class spent time and will spend additional time in the future speaking with representatives; researching and monitoring accounts; researching and monitoring credit history; responding to identity theft incidents; purchasing identity protection;

loss of value of their PII; the loss of personal and financial security; the loss of the opportunity to timely attempt to protect themselves from the breach; the ongoing threat of the invasion of their personal information and the risk that poses to their health and welfare and personal security; and annoyance, interference, and inconvenience, as a result of the Data Breach. Further, they suffer from a present, immediate and imminent and continuing risk of harm, including but not limited to, the serious and immediate risk of fraud and identity theft.

125. StockX's actions and failures to act when required have caused Plaintiffs and the Class to suffer harm and face the significant and imminent risk of future harm, including:

- a) theft of their PII;
- b) costs associated with researching the scope and nature of the breach and of responding to the Data Breach and attendant risks and harm in light of StockX's misinformation campaign;
- c) costs associated with the detection and prevention of identity theft and unauthorized use of their PII, including costs associated with credit monitoring, password protection, freezing/unfreezing of credit, obtaining credit reports, and penalties resulting from frozen credit;
- d) unauthorized access to and misuse of their online accounts;

- e) lowered credit scores resulting from credit inquiries following fraudulent activities;
- f) costs, including opportunity costs, associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the StockX Data Breach—including finding fraudulent charges and enrolling in and purchasing credit monitoring and identity theft protection services;
- g) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals;
- h) damages to and diminution in value of their PII entrusted, directly or indirectly, to StockX with the mutual understanding that StockX would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;
- i) loss of the benefit of the bargain with StockX to provide adequate and reasonable data security – i.e., the difference in value between what Plaintiffs should have received from StockX when StockX represented Plaintiff's Personal Information would be protected by reasonable data

security and StockX's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiffs' Personal Information; and

- j) continued risk of exposure to hackers and thieves of their PII, which remains in StockX's possession and is subject to further breaches so long as StockX fails to undertake appropriate and adequate measures to protect Plaintiffs and the Class.

126. Consequently, Plaintiffs and the Class are at an imminent risk of fraud, criminal misuse of their PII, and identity theft for years to come as result of the Data Breach and StockX's deceptive and unconscionable conduct. Plaintiffs bring this action on behalf of adults and minors similarly situated both across the United States and within their State or Territory of residence.

CLASS ACTION ALLEGATIONS

127. Class certification is appropriate under Fed. R. Civ. P. 23(a) and (b)(1), (b)(2), and/or (b)(3).

128. **Nationwide Class:** All individuals in the United States whose PII was obtained or maintained by StockX and compromised as a result of the StockX Data Breach described herein.

129. **Nationwide Adult Subclass:** All adult individuals in the United States whose PII was obtained or maintained by StockX and compromised as a result of the StockX Data Breach described herein.

130. **Nationwide Minor Subclass:** All minor individuals in the United States whose PII was obtained or maintained by StockX and compromised as a result of the StockX Data Breach described herein, as well as all individuals in the United States who provided their PII to StockX while they were minors and had their PII compromised as a result of the StockX Data Breach described herein.

131. **State Subclasses for Adults and Minor Plaintiffs:** In the alternative, Plaintiffs request certification of sub-classes of persons in each and every State whose PII was obtained or maintained by StockX and compromised as a result of the StockX Data Breach:

- a) Kansas - All adult persons who are citizens of Kansas and whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach.
- b) Kansas - All minor persons who are citizens of Kansas and whose PII was obtained or maintained by Stock X and compromised as a result of the StockX data breach.

- c) New York - All adult persons who are citizens of New York and whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach.
- d) New York - All minor persons who are citizens of New York and whose PII was obtained or maintained by Stock X and compromised as a result of the StockX data breach.
- e) New Jersey - All adult persons who are citizens of New Jersey and whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach.
- f) New Jersey - All minor persons who are citizens of New Jersey and whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach.
- g) Georgia - All adult persons who are citizens of Georgia and whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach.
- h) Georgia - All minor persons who are citizens of Georgia and whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach.

- i) California - All adult persons who are citizens of Georgia and whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach.
- j) California - All minor persons who are citizens of California and whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach.
- k) Florida - All adult persons who are citizens of Florida and whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach.
- l) Florida - All minor persons who are citizens of Florida and whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach.

132. The Nationwide Class, Nationwide Adult Subclass, the Nationwide Minor Subclass, and the Kansas, New York, New Jersey, Georgia, California, and Florida subclasses are collectively referred to herein as the “Class.”

133. Excluded from the Class are StockX, any entity in which StockX has a controlling interest, and StockX’s officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, members of

their judicial staff, and any judge sitting in the presiding court system who may hear an appeal of any judgment entered.

134. **Numerosity (FRCP 23(a)(1)):** The class satisfies the numerosity requirement because it is composed of millions of persons, in numerous locations. The number of class members is so large that joinder of all its members is impracticable. Affected consumer's names and addresses are available from StockX's records, and class members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include electronic mail, U.S. Mail, internet notice, and/or published notice.

135. **Commonality and Predominance (FRCP 23(a)(2) and 23(b)(3)):** There are questions of law and fact common to the Class, and these questions predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to:

- a) Whether the Data Breach constitutes a breach of the data-security commitments and obligations to protect and safeguard PII made to the Class by StockX in its Privacy Policy;
- b) Whether StockX breached its duties to protect the PII of Plaintiffs and the Class by failing to provide adequate data security;

- c) Whether StockX acted with negligence, recklessness and/or intent with respect to the Class and the safety, value, and security of the Class's PII when it falsely advised the Class that a password reset was required because of a "system update," not a Data Breach, which StockX knew to be the case at the time of its statements;
- d) Whether StockX was negligent, reckless or intentionally indifferent in its representations to the Class concerning its security protocols;
- e) Whether StockX omitted or misrepresented material facts regarding the security of its computer and data storage systems and their inability to protect vast amounts of consumer data, including Plaintiffs' and class members' PII;
- f) Whether StockX failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard its customers' PII;
- g) Whether StockX's conduct amounted to violations of state consumer protection statutes, and/or state data breach statutes;
- h) Whether StockX's conduct and practices described herein amount to acts of intrusion upon seclusion under the laws of the "Intrusion Upon Seclusion States" defined below;

- i) Whether StockX was negligent, reckless, and/or intentionally deceptive in making misrepresentations to the Class when it falsely advised the Class that a password reset was required because of a “system update,” not a Data Breach, which StockX knew to be the case at the time of its statements;
- j) Whether StockX was negligent in establishing, implementing, and following security protocols;
- k) Whether StockX failed to abide by all applicable legal requirements (including relevant state law requirements) and industry standards concerning the privacy and confidentiality of the Class members’ PII;
- l) Whether the Class members’ PII was compromised and exposed as a result of the Data Breach; and
- m) Whether the Class members are entitled to compensatory damages;

136. **Typicality (FRCP 23(a)(3)):** Plaintiffs’ claims are typical of the claims of the members of the Class because Plaintiffs’ claims, and the claims of all Class members, arise out of the same conduct, policies, and practices of StockX, as alleged herein, and all members of the Class are similarly affected by StockX’s wrongful conduct and the Data Breach described herein.

137. **Adequacy of Representation (FRCP 23(a)(4)):** Plaintiffs will fairly and adequately represent the Class and have retained counsel competent in the prosecution of class action litigation; Data Breach litigation; data privacy and cybersecurity law; and technical I.T. concepts, practices, and theory. Plaintiffs have no interests antagonistic to those of other members of the Class. Plaintiffs are committed to the vigorous prosecution of this action and anticipate no difficulty in the management of this litigation as a class action.

138. Class action status in this action is warranted under Rule 23(b)(1)(A) because prosecution of separate actions by the members of the Class would create a risk of establishing incompatible standards of conduct for Defendants. Class action status is also warranted under Rule 23(b)(1)(B) because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

139. Certification under Rule 23(b)(2) is warranted because Defendants acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive, declaratory, or other appropriate equitable relief with respect to the Class as a whole.

140. Certification under Rule 23(b)(3) is appropriate because questions of law or fact common to members of the Class predominate over any questions affecting only individual members, and class action treatment is superior to the other methods for the fair and efficient adjudication of this controversy. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs and class members may not be sufficient to justify individual litigation. Individual litigation to redress StockX's wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION AND CLAIMS FOR RELIEF

COUNT I — Negligence

(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, the Nationwide Minor Subclass, and State Subclasses)

141. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

142. This count is brought on behalf of all Class members.

143. StockX owed a duty to Plaintiffs and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing their PII that StockX collected.

144. Plaintiffs I.C., M.S., and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of StockX users, as documented in academic and government-issued materials, by experts in the field, and by the media.

145. StockX owed a duty to Plaintiffs and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing their PII that StockX collected, and StockX was aware of the vulnerability and damage that would be suffered by Plaintiffs and the Class in the event of a Data Breach.

146. StockX owed a heightened duty to Plaintiffs I.C., M.S., and the Nationwide Minor Subclass to use and exercise reasonable and due care in obtaining, retaining, and securing their PII that StockX collected, and StockX was aware of the heightened vulnerability and damage that would be suffered by I.C., M.S., and the Nationwide Minor Subclass in the event of a Data Breach.

147. StockX owed a duty to Plaintiffs and the Class to provide security, consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII that StockX collected.

148. StockX owed a heightened duty to Plaintiffs I.C., M.S., and the Nationwide Minor Subclass to provide security, consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the minors' PII that StockX collected.

149. StockX owed a duty to Plaintiffs and the Class to implement processes to quickly detect a Data Breach, to timely act on warnings about Data Breaches, and to inform the Class of a Data Breach as soon as possible after it is discovered.

150. StockX owed a heightened duty to Plaintiffs I.C., M.S., and the Nationwide Minor Subclass to implement processes to quickly detect a Data Breach, to timely act on warnings about Data Breaches, and to inform the Class of a Data Breach as soon as possible after it is discovered.

151. StockX owed a duty of care to Plaintiffs and the Class because they were foreseeable and probable victims of any inadequate data security practices.

152. StockX owed a heightened duty to Plaintiffs I.C., M.S., and the Nationwide Minor Subclass because they were foreseeable and probable victims of any inadequate data security practices.

153. StockX solicited, gathered, and stored the PII provided by Plaintiffs and the Class.

154. StockX knew or should have known it inadequately safeguarded this information.

155. StockX knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiffs and the Class, and StockX was therefore charged with a duty to adequately protect this critically sensitive information.

156. StockX had a special relationship with Plaintiffs and the Class. Plaintiffs' and the Class's willingness to entrust StockX with their PII was predicated on the understanding that StockX would take adequate security precautions. Plaintiffs were required to provide their PII to StockX in order to transact on its e-commerce platform. Moreover, only StockX had the ability to protect its systems and the PII it stored on them from attack.

157. StockX's own conduct also created a foreseeable risk of harm to Plaintiffs and the Class and their financial information. StockX's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of Data Breach.

158. StockX breached its duties to Plaintiffs and the Class by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the financial information of Plaintiffs and the Class.

159. StockX breached its heightened duties to Plaintiffs I.C., M.S., and the Nationwide Minor Subclass by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the financial information of Plaintiffs I.C., M.S., and the Nationwide Minor Subclass.

160. StockX breached its duties to Plaintiffs and the Class by creating a foreseeable risk of harm through the misconduct previously described.

161. StockX breached its heightened duties to Plaintiffs I.C., M.S., and the Nationwide Minor Subclass by creating a foreseeable risk of harm through the misconduct previously described.

162. StockX breached the duties it owed to Plaintiffs and the Class by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

163. StockX breached its heightened duties to Plaintiffs I.C., M.S., and the Nationwide Minor Subclass by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

164. StockX breached the duties it owed to Plaintiffs and the Class by failing to properly implement technical systems or security practices to detect that its system(s) were compromised and/or being compromised.

165. StockX breached its heightened duties to Plaintiffs I.C., M.S., and the Nationwide Minor Subclass by failing to properly implement technical systems or security practices to detect that its system(s) were compromised and/or being compromised.

166. StockX breached the duties it owed to Plaintiffs and the Class by failing to timely, adequately, and accurately disclose that Plaintiffs' and the Class members' PII had been improperly stolen, acquired, or accessed.

167. StockX breached its heightened duties to Plaintiffs I.C., M.S., and the Nationwide Minor Subclass by failing to timely, adequately, and accurately disclose that Plaintiffs I.C., M.S., and the Nationwide Minor Subclass's PII had been improperly stolen, acquired, or accessed.

168. StockX breached its affirmative duty to timely disclose the unauthorized access and theft of the financial and sensitive information to Plaintiffs and the Class so that Plaintiffs and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their financial and sensitive information.

169. Moreover, StockX breached its heightened affirmative duty to timely disclose the unauthorized access and theft of the PII to Plaintiffs I.C., M.S., and the Nationwide Minor Subclass so that Plaintiffs I.C., M.S., and the Nationwide Minor Subclass can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their financial and sensitive information.

170. StockX breached its duty to notify Plaintiffs and the Class by failing to provide Plaintiffs and the Class information regarding the breach until August 3, 2019. To date, StockX has not provided sufficient information to Plaintiffs and the Class regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

171. As a direct and proximate result of StockX's negligent conduct, Plaintiffs have suffered a drastic increase in their risk of identity theft, relative to both the time period before the breach, as well as to the risk borne by the general public.

172. As a direct and proximate result of StockX's negligent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial. Such injuries include, but are not limited to, one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm;

loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing online accounts, bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT II –Misrepresentation

(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, the Nationwide Minor Subclass, and State Subclasses)

173. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

174. This count is brought on behalf of all Class members.

175. Through its Privacy Policy and other actions and representations, StockX held itself out to Plaintiffs and the Class as possessing and maintaining adequate data security measures and systems that were sufficient to protect the PII belonging to Plaintiffs and the Class.

176. StockX owed a duty to Plaintiffs and the Class to communicate accurate information about its compliance with the representations made in its Privacy Policy and about any material weaknesses in its data security systems and procedures.

177. StockX knew or should have known that it was not in compliance with the representations made in its Privacy Policy.

178. StockX knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith and common decency required it to disclose to Plaintiffs and the Class.

179. Neither Plaintiffs nor the Class could have known or discovered the material weaknesses in StockX's data security practices.

180. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to Plaintiffs and the Class.

181. StockX also failed to exercise reasonable care when it falsely conveyed information to Plaintiffs and the Class on August 1, 2019, relating to the underlying need for Plaintiffs and the Class to reset their passwords, which misrepresentation failed to sufficiently convey the facts underlying the actual need for a password reset; failed to instill the urgency of the need to reset their passwords immediately; provided the thieves of the stolen information with additional time and cover to further purloin

and re-sell the stolen PII belonging to Plaintiffs and the Class; provided the thieves and the purchasers of the stolen information with an opportunity to directly defraud Plaintiffs and the Class; and failed to adequately apprise Plaintiffs and the Class of the fact that their PII was compromised and in imminent jeopardy of falling further into the hands of cyber criminals.

182. StockX also failed to exercise reasonable care when it failed to timely communicate information concerning the Data Breach that it knew, or should have known, compromised PII of Plaintiffs and the Class.

183. Plaintiffs and the Class relied on StockX's representations, or lack thereof, when they provided their PII to StockX.

184. Despite its knowledge of the Data Breach and the imminent danger the PII theft posed, StockX failed to timely and forthrightly advise Plaintiffs and the Class of the breach; instead, StockX falsely advised Plaintiffs and the Class that a password reset was necessary because of "system upgrades."

185. In conjunction, and simultaneous with its misrepresentations relating to the need for Plaintiffs and the Class to reset their passwords, StockX intentionally failed to communicate to Plaintiffs and the class material facts relating to the Data Breach, the theft of their PII, the urgency with which Plaintiffs and the Class needed to update their passwords, the concurrent and urgent need for Plaintiffs and the Class

to protect and safeguard their data, and other measures needed in light of the Data Breach.

186. Plaintiffs and the Class justifiably relied on StockX's misrepresentations and StockX's intentional withholding of material facts, suffered injuries as a result, and were damaged as discussed herein and as will be proven at trial.

187. As a direct and proximate result of StockX's negligent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial. Such injuries include, but are not limited to, one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing online accounts, bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT III – Negligence Per Se – FTC Act

**(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass,
the Nationwide Minor Subclass, and State Subclasses)**

188. Plaintiffs incorporates and reallege all allegations above as if fully set forth herein.

189. This count is brought on behalf of all Class members.

190. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair...practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as StockX of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of StockX’s duty.

191. StockX violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII; by failing to comply with applicable industry standards; by falsely representing to its users and the public the nature and scope of the Data Breach and the need for password resets; and by unduly delaying reasonable notice of the actual breach. StockX’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of a Data Breach, and the foreseeable consequences of misleading its users and the public.

192. StockX’s violation of Section 5 of the FTC Act constitutes negligence per se.

193. Plaintiffs and the Class are within the category of persons the FTC Act was intended to protect.

194. The harm that occurred as a result of the Data Breach described herein and in the various media reports detailing StockX's deception relating to the Data Breach is the type of harm the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of defendants' failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and class members.

195. As a direct and proximate result of StockX's negligent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial. Such injuries include, but are not limited to, one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing online accounts, bank statements,

payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT IV – Fraud and Silent Fraud

(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, the Nationwide Minor Subclass, and State Subclasses)

195. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

196. This count is brought on behalf of all Class members.

197. StockX knew that data belonging to Plaintiffs and the Class had been stolen prior to its false “system update” email on August 1, 2019. This knowledge was of material importance relating to the safety, value, and security of the PII belonging to Plaintiffs and the Class.

198. Plaintiffs and the Class did not know about the theft of their PII from StockX, nor could they have discovered such information by exercise of reasonable diligence.

199. StockX was under an obligation to forthrightly and promptly communicate the pertinent facts relating to the Data Breach to Plaintiffs and the Class to permit them to undertake appropriate protective measures to mitigate the harm

caused by StockX's failure to adequately protect the data and to reasonably safeguard their identities, livelihood, and safety.

200. Despite its knowledge of the Data Breach and the imminent danger the PII theft posed, StockX failed to timely and forthrightly advise Plaintiffs and the Class of the breach; instead, StockX falsely advised Plaintiffs and the Class that a password reset was necessary because of "system upgrades."

201. In conjunction, and simultaneous with its misrepresentations relating to the need for Plaintiffs and the Class to reset their passwords, StockX intentionally failed to communicate to Plaintiffs and the class material facts relating to the Data Breach, including how Plaintiffs' and Class Members' PII was improperly procured; the theft of Plaintiffs' and Class Members' PII; the inadequacy of StockX's measures to secure Plaintiffs' and Class Members' PII or otherwise prevent the theft of said data; StockX's failure to determine or otherwise deduce that Plaintiffs' and Class Members' PII had been compromised; the urgency with which Plaintiffs and the Class needed to update their passwords; the concurrent and urgent need for Plaintiffs and the Class to protect and safeguard their data; and other measures needed in light of the Data Breach.

202. Plaintiffs and the Class justifiably relied on StockX's misrepresentations and StockX's intentional withholding of material facts. As a direct and proximate

result of StockX's fraudulent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial. Such injuries include, but are not limited to, one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing online accounts, bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT V – Violation of State Data Breach Statutes

(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, the Nationwide Minor Subclass, and State Subclasses residing in states with applicable Data Breach statutes)

203. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

204. This count is brought on behalf of all Class members.

205. StockX is a business that owns, maintains, and licenses PII, and computerized data including PII, about Plaintiffs and Class members.

206. StockX is in possession of PII belonging to Plaintiffs and the Class and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

207. StockX failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by the laws of the states described herein.

208. StockX, knowing and/or reasonably believing that Plaintiffs and Class members PII was acquired by unauthorized persons during the Data Breach, further failed to provide reasonable and timely notice of the Data Breach to Plaintiffs and the Class as required by following Data Breach statutes.

209. StockX's failure to adequately safeguard Plaintiffs' and the Class Members' PII and provide timely and accurate notice of the Data Breach violated the following state Data Breach statutes:

- a) Alaska Stat. Ann. § 45.48.010(a), et seq.;
- b) Ark. Code Ann. § 4-110-105(a), et seq.;
- c) Cal. Civ. Code § 1798.83(a), et seq.;
- d) Colo. Rev. Stat. Ann § 6-1-716(2), et seq.;
- e) Conn. Gen. Stat. Ann. § 36a-701b(b), et seq.;

- f) Del. Code Ann. Tit. 6 § 12B-102(a), et seq.;
- g) D.C. Code § 28-3852(a), et seq.;
- h) Fla. Stat. Ann. § 501.171(4), et seq.;
- i) Ga. Code Ann. § 10-1-912(a), et seq.;
- j) Haw. Rev. Stat. § 487N-2(a), et seq.;
- k) Idaho Code Ann. § 28-51-105(1), et seq.;
- l) Ill. Comp. Stat. Ann. 530/10(a), et seq.;
- m) Iowa Code Ann. § 715C.2(1), et seq.;
- n) Kan. Stat. Ann. § 50-7a02(a), et seq.;
- o) Ky. Rev. Stat. Ann. § 365.732(2), et seq.;
- p) La. Rev. Stat. Ann. § 51:3074(A), et seq.;
- q) Md. Code Ann., Commercial Law § 14-3504(b), et seq.;
- r) Mass. Gen. Laws Ann. Ch. 93H § 3(a), et seq.;
- s) Mich. Comp. Laws Ann. § 445.72(1), et seq.;
- t) Minn. Stat. Ann. § 325E.61(1)(a), et seq.;
- u) Mont. Code Ann. § 30-14-1704(1), et seq.;
- v) Neb. Rev. Stat. Ann. § 87-803(1), et seq.;
- w) Nev. Rev. Stat. Ann. § 603A.220(1), et seq.;
- x) N.H. Rev. Stat. Ann. § 359-C:20(1)(a), et seq.;
- y) N.J. Stat. Ann. § 56:8-163(a), et seq.;
- z) N.C. Gen. Stat. Ann. § 75-65(a), et seq.;
- aa) N.D. Cent. Code Ann. § 51-30-02, et seq.;
- bb) Okla. Stat. Ann. Tit. 24 § 163(A), et seq.;
- cc) Or. Rev. Stat. Ann. § 646A.604(1), et seq.;
- dd) R.I. Gen. Laws Ann. § 11-49.3-4(a)(1), et seq.;

- ee) S.C. Code Ann. § 39-1-90(A), et seq.;
- ff) Tenn. Code Ann. § 47-18-2107(b), et seq.;
- gg) Tex. Bus. & Com. Code Ann. § 521.053(b), et seq.;
- hh) Utah Code Ann. § 13-44-202(1), et seq.;
- ii) Va. Code. Ann. § 18.2-186.6(B), et seq.;
- jj) Wash. Rev. Code Ann. § 19.255.010(1), et seq.;
- kk) Wis. Stat. Ann. § 134.98(2), et seq.; and
- ll) Wyo. Stat. Ann. § 40-12-502(a), et seq.

210. As a result of StockX's failure to reasonably safeguard the PII belonging to Plaintiffs and the Class, and StockX's failure to provide reasonable and timely notice of the Data Breach to Plaintiffs and the Class, Plaintiffs and the Class have been injured and sustained damages as described herein, continue to suffer harm as detailed above, are subject to the continued risk of exposure of their PII in StockX's possession, and are entitled to any and all damages and equitable relief allowed by law.

COUNT VI – Violation of State Consumer Protection Statutes
(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, the Nationwide Minor Subclass, and State Subclasses)

211. Plaintiffs reallege and incorporate by reference the allegations contained in the above paragraphs, as if fully set forth herein.

212. This count is brought on behalf of all Class members.

213. Plaintiffs and Class members are consumers who purchased products from, and/or transacted with, StockX primarily for personal, family or household purposes.

214. StockX is a “person” as defined in the relevant state consumer statutes.

215. StockX engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiffs and Class members. StockX is engaged in, and its acts and omissions affect, trade and commerce.

216. StockX’s acts, practices and omissions were done in the course of StockX’s business of marketing, facilitating, offering for sale, and selling goods and services throughout the United States.

217. StockX’s unlawful, unfair, deceptive, fraudulent and/or unconscionable acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the

e-commerce industry, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class members' PII, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class Members' PII, including by implementing and maintaining reasonable security measures
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and the Class members' PII;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' Class members' PII; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII.

218. By engaging in such conduct and omissions of material facts, StockX has violated state consumer laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that

they do not have,” representing that “goods and services are of a particular standard, quality or grade, if they are of another”, and/or “engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding”; and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

219. StockX’s representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of StockX’s data security and ability to protect the confidentiality of Plaintiffs’ and Class Members’ PII.

220. StockX intentionally, knowingly, and maliciously misled Plaintiffs and Class Members and induced them to rely on its misrepresentations and omissions.

221. Had StockX disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, StockX would have been forced to adopt reasonable data security measures and comply with the law. Instead, StockX received, maintained, and compiled Plaintiffs’ and Class Members’ PII as part of the services StockX provided and for which Plaintiffs and Class members paid without advising Plaintiffs and Class members that StockX’s data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs and Class Members’ PII. Accordingly, Plaintiffs and the Class Members acted reasonably in

relying on StockX's misrepresentations and omissions, the truth of which they could not have discovered.

222. Past breaches within the e-commerce industry put StockX on notice that its security and privacy protections were inadequate.

223. StockX's practices were also contrary to public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures.

224. The harm these practices caused to Plaintiffs and the Class members had no utility and only caused harm to Plaintiffs and the Class Members.

225. The injuries, damages, and losses, including to their money, property, and/or right to privacy suffered by Plaintiffs and Class members as a direct result of StockX's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices as set forth in this Complaint include, without limitation:

- a. unauthorized charges on their debit and credit card accounts;
- b. theft of their personal and financial information;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

- d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;
- e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the StockX Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the StockX Data Breach;
- f. the imminent, ongoing, and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and being already misused via the sale of consumers' information on the dark web;

- g. damages to and diminution in value of their personal and financial information entrusted to StockX for the purpose of purchasing products from StockX and with the understanding that StockX would safeguard their data against theft and not allow access and misuse of their data by others;
- h. money paid for products purchased from StockX during the period of the StockX breach in that Plaintiffs and Class members would not have purchased from StockX had StockX disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had StockX provided timely and accurate notice of the StockX Data Breach;
- i. overpayments made to StockX for transactions during the StockX Data Breach in that a portion of the price for such products paid by Plaintiffs and the Class members to StockX was for the costs of StockX providing reasonable and adequate safeguards and security measures to protect customers' financial and personal data, which StockX failed to do and, as a result, Plaintiffs and Class members did not receive what they paid for and were overcharged by StockX; and

- j. the continued risk to their personal information, which remains in the possession of StockX and which is subject to further breaches so long as StockX fails to undertake appropriate and adequate measures to protect data in its possession.

226. StockX's conduct described in this Complaint, including without limitation, StockX's failure to maintain adequate computer systems and data security practices to safeguard customers' PII, StockX's failure to disclose the material fact that it did not have adequate computer systems and safeguards to adequately protect users' PII, StockX's failure to provide timely and accurate notice to Consumer Plaintiffs and Class members of the material fact of the StockX Data Breach, and StockX's continued acceptance of Consumer Plaintiffs' and Class members' PII, including credit and banking information for transactions on StockX after StockX knew or should have known of the Data Breach, constitute unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation of the following state consumer statutes:

- a. The Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5(5), (7) and (27), *et seq.*;
- b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;
- c. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), *et seq.*;

- d. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.*, and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq.*
- e. The Colorado Consumer Protection Act, Col. Rev. Stat. Ann. §§ 6-1-105(1)(b), (c), (e) and (g), *et seq.*;
- f. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), *et seq.*;
- g. The Delaware Deceptive Trade Practices Act, Del. Code Ann. Title 6, § 2532(5) and (7), *et seq.*, and the Delaware Consumer Fraud Act, Del. Code Ann. Title 6 § 2513, *et seq.*;
- h. The District of Columbia Consumer Protection Act, D.C. Code §§ 28-3904(a), (d), (e), (f) and (r), *et seq.*;
- i. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq.*;
- j. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (5) and (7), *et seq.*;
- k. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), *et seq.*; and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq.*;
- l. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), *et seq.*; and Idaho Code § 48-603C, *et seq.*;
- m. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq.*, and the Illinois Uniform Deceptive Trades Practices Act, 815 Ill. Stat. § 510/2(a)(5), (7) and (12), *et seq.*;

- n. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), et seq.;
- o. The Iowa Consumer Fraud Act, I.C.A. §§ 714H.3 and 714H.5, et seq., Consumer Plaintiffs have obtained the approval of the Iowa Attorney General for filing this class action lawsuit as provided under I.C.A. § 714H.7;
- p. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), et seq.;
- q. The Kentucky Consumer Protection Act, K.R.S. § 367.170(1) and (2), et seq.;
- r. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), et seq.;
- s. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), et seq.;
- t. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§ 1212(1)(E) and (G), et seq., and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, et seq.;
- u. The Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), et seq.;
- v. The Michigan Consumer Protection Act, M.C.P.L.A. § 445.903(1)(c)(e),(s) and (cc), et seq.;
- w. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), et seq., the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a);

- x. The Mississippi Consumer Protection Act, Miss. Code Ann. §§ 75-24-5(1), (2)(e) and (g), *et seq.*;
- y. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq.*;
- z. The Montana Unfair Trade Practices and Consumer Protection Act, MCA §§ 30-14-103, *et seq.*;
- aa. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq.*;
- bb. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(v) and (vii), *et seq.*;
- cc. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;
- dd. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, *et seq.*;
- ee. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5) and (7), *et seq.*;
- ff. New York Business Law, N.Y. Gen. Bus. Law § 349(a);
- gg. The North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), *et seq.*;
- hh. The North Dakota Unlawful Sales or Advertising Practices Act, N.D. Cent. Code § 51-15-02, *et seq.*;
- ii. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.02(A) and (B)(1) and (2), *et seq.*

- jj. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. § 753(5), (7) and (20), *et seq.*; and the Oklahoma Deceptive Trade Practices Act, 78 Okl. Stat. Ann. § 53(A)(5) and (7), *et seq.*;
- kk. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(e)(g) and (u), *et seq.*;
- ll. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq.*;
- mm. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), *et seq.*;
- nn. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), *et seq.*;
- oo. The South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1), *et seq.*;
- pp. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a) and (b)(5) and (7);
- qq. The Texas Deceptive Trade Practices- Consumer Protection Act, V.T.C.A., Bus. & C. § 17.46(a), (b)(5) and (7), *et seq.*;
- rr. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1) and (2)(a) and (b);
- ss. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), *et seq.*;
- tt. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(5)(6) and (14), *et seq.*;
- uu. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq.*;

- vv. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq.*;
- ww. The Wisconsin Deceptive Trade Practices Act, W.S.A. § 100.20(1), *et seq.*; and
- xx. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-105(a), (i), (iii) and (xv), *et seq.*

227. Written pre-suit demand is being made at the time of filing this Consolidated Complaint for Plaintiffs residing in states providing for such demands. StockX has long had notice of Plaintiffs' allegations, claims and demands including from the filing of numerous actions by various consumer plaintiffs against StockX arising from the Data Breach, the first of which was filed on August 6, 2019.

228. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; statutory damages; declaratory and injunctive relief, including an injunction barring StockX from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is allowable by law.

COUNT VII – Intrusion Upon Seclusion

(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, the Nationwide Minor Subclass, and State Subclasses who reside in Intrusion Upon Seclusion States)

229. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

230. This count is brought on behalf of all Class members.

231. Plaintiffs bring this claim on behalf of persons who reside in Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia; and any other state that recognizes a claim for intrusion upon seclusion under the facts and circumstances alleged above (the “Intrusion Upon Seclusion States”).

232. Plaintiffs had a reasonable expectation of privacy in the PII that StockX mishandled.

233. By failing to keep Plaintiffs’ Private Information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, StockX invaded Plaintiffs’ and the Class Members’ privacy and/or caused Plaintiffs’ and Class Members’ privacy to be invaded by:

- a) Intruding and/or allowing intrusion into Plaintiffs’ and the Class Members’ private affairs in a manner that would be highly offensive to a reasonable person; and

- b) Publicizing and/or allowing or otherwise facilitating the publication of private facts about the Plaintiffs and the Class Members, which is highly offensive to a reasonable person.

234. StockX knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' position would consider StockX's actions highly offensive.

235. StockX invaded Plaintiffs' right to privacy and intruded into Plaintiffs' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

236. As a proximate result of such misuse and disclosures, Plaintiffs' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. StockX's conduct amounted to a serious invasion of Plaintiffs' protected privacy interests.

237. In failing to protect Plaintiffs' Private Information, and in misusing and/or disclosing their Private Information, StockX has acted with malice and oppression and in conscious disregard of Plaintiffs' and the Class Members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its many millions of users. The Plaintiff, therefore, seek an award

of damages, including punitive damages, and/or any equitable relief allowed by law on behalf of Plaintiffs and the Class.

COUNT VIII – Unjust Enrichment

(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, the Nationwide Minor Subclass, and State Subclasses)

238. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

239. This count is brought on behalf of all Class members.

240. Plaintiffs and the Class have an interest, both equitable and legal, in their PII that was collected and maintained by StockX. This PII was conferred on StockX directly by Plaintiffs and the Class themselves.

241. StockX has benefitted by the conferral upon it of the PII pertaining to Plaintiffs and the Class and by its ability to retain and use that information. StockX understood that it was in fact so benefitted.

242. StockX also understood and appreciated that the PII pertaining to Plaintiffs and the Class was private and confidential and its value depended upon StockX maintaining the privacy and confidentiality of that PII.

243. But for StockX's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and the Class would not have transferred PII to StockX or entrusted their PII to StockX, and StockX would have been deprived of the

competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining customers and users of its platform, gaining the reputational advantages conferred upon it by Plaintiffs and the Class, collecting excessive advertising and sales revenues, monetary savings resulting from failure to reasonably upgrade and maintain IT infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

244. As a result of StockX's wrongful conduct as alleged in this Complaint (including, among other things, its deception of Plaintiff, the Class, its users in general, and the public relating to the nature and scope of the Data Breach; its utter failure to employ adequate data security measures; its continued maintenance and use of the PII belonging to Plaintiffs and the Class without having adequate data security measures; and its other conduct facilitating the theft of that PII) StockX has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class.

245. StockX's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members' sensitive PII, while at the same time failing to maintain that information secure from intrusion.

246. Under the common law doctrine of unjust enrichment, it is inequitable for StockX to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and the Class in an unfair and unconscionable manner. StockX's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

247. The benefit conferred upon, received, and enjoyed by StockX was not conferred officiously or gratuitously by Plaintiffs and the Class, StockX had knowledge and appreciation of the benefit conferred by Plaintiffs and the Class as well as its retention of the benefit, and it would be inequitable and unjust for StockX to retain the benefit.

248. StockX is therefore liable to Plaintiffs and the Class for restitution in the amount of the benefit conferred on StockX as a result of its wrongful conduct, including specifically the value to StockX of the PII that was stolen in the StockX Data Breach and the profits StockX is receiving from the use and sale of that information.

COUNT IX – Bailment

(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, the Nationwide Minor Subclass, and State Subclasses)

249. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

250. This count is brought on behalf of all Class members.

251. Plaintiffs and Class members delivered their personal and financial information to StockX for the exclusive purpose of utilizing the StockX platform, including to purchase and sell items on StockX.

252. In delivering their personal and financial information to StockX, Plaintiffs and Class members intended and understood that StockX would adequately safeguard their personal and financial information.

253. StockX accepted possession of Plaintiffs' and Class members' personal and financial information for the purpose of facilitating transactions by Plaintiffs and Class members on the StockX website.

254. By accepting possession of Plaintiffs' and Class members' personal and financial information, StockX understood that Consumer Plaintiffs and Class members reasonably expected StockX to adequately safeguard their personal and financial information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

255. During the bailment (or deposit), StockX owed a duty to Plaintiffs and Class members to exercise reasonable care, diligence and prudence in protecting their personal and financial information.

256. StockX breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and Class members' personal and financial information.

257. StockX further breached its duty to safeguard Plaintiffs' and Class members' personal and financial information by failing to timely and accurately notify them that their information had been compromised as a result of the StockX Data Breach.

258. StockX failed to return, purge or delete the personal and financial information of Consumer Plaintiffs and members of the Class at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

259. As a direct and proximate result of StockX's breach of its duty, Plaintiffs and Class members were injured and suffered consequential damages that were reasonably foreseeable to StockX.

260. As a direct and proximate result of StockX's breach of its duty, the PII of Plaintiffs and Class members entrusted to StockX during the bailment (or deposit) was damaged and its value diminished.

COUNT X – Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, the Nationwide Minor Subclass, and State Subclasses)

261. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

262. This count is brought on behalf of all Class members.

263. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

264. An actual controversy has arisen in the wake of the StockX Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether StockX is currently maintaining data security measures adequate to protect Plaintiffs and the Class from further Data Breaches that compromise their PII. Plaintiffs allege that StockX's data security measures remain inadequate.

265. Plaintiffs and the Class members continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

266. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that StockX continues to owe a legal duty to secure

consumers' PII and to timely notify consumers of any Data Breach and that StockX is required to establish and implement data security measures that are adequate to secure consumers' PII.

267. The Court also should issue corresponding prospective injunctive relief requiring StockX to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

268. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury, and Plaintiffs and the Class lack an adequate legal remedy. The threat of another StockX Data Breach is real, immediate, and substantial. If another breach at StockX occurs, Plaintiffs will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

269. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to StockX if an injunction is issued. Among other things, if another massive Data Breach occurs at StockX, Plaintiffs will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to StockX of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and StockX has a pre-existing legal obligation to employ such measures.

270. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another Data Breach at StockX, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of members of the Class, as applicable, respectfully requests that the Court enter judgment in their favor and against StockX, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure, and such sub-classes as the Court shall deem proper and just; declare that Plaintiffs are proper class representatives; and appoint Interim Class Counsel as Class Counsel;
2. That Plaintiffs be granted the declaratory relief sought herein;
3. That the Court grant permanent injunctive relief to prohibit StockX from continuing to engage in the unlawful acts, omissions, and practices described herein;
4. That the Court award Plaintiffs and the Class members compensatory, and monetary damages in an amount to be determined at trial;
5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That the Court award to Plaintiffs the costs and disbursements of the action, along with attorneys' fees, costs, and expenses;
7. That the Court award pre- and post-judgment interest;
8. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and
9. That the Court grant all such other legal and equitable relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Dated: May 11, 2020

Respectfully submitted,

/s/ E. Powell Miller

E. Powell Miller (P39487)

Sharon S. Almonrode (P33938)

Melvin B. Hollowell (P37834)

William Kalas (P82113)

THE MILLER LAW FIRM, P.C.

950 W. University Dr., Suite 300

Rochester, Michigan 48307

Telephone: (248) 841-2200

Fax: (248) 652-2852

epm@millerlawpc.com

ssa@millerlawpc.com

wk@millerlawpc.com

*Interim Lead Counsel for Plaintiffs and the
Class*

Scott C. Nehrbass
Daniel J. Buller
FOULSTON SIEFKIN LLP
32 Corporate Woods, Suite 600
9225 Indian Creek Parkway
Overland Park, KS 66210-2000
Tel: (913) 253-2144
Fax: (866) 347-1472
snehrbass@foulston.com
dbuller@foulston.com

Boyd A. Byers
FOULSTON SIEFKIN LLP
1551 N. Waterfront Parkway, Suite 100
Wichita, Kansas 67206-4466
Tel: (316) 291-9796
Fax: (866) 559-6541
bbyers@foulston.com

Patrick Cafferty (P35613)
**CAFFERTY CLOBES MERIWETHER
& SPRENGEL LLP**
220 Collingwood Drive, Suite 130
Ann Arbor, Michigan 48103
Telephone: (734) 769-2144
Facsimile: (312) 782-4485
pcafferty@caffertyclobes.com

Daniel O. Herrera, Esq.
**CAFFERTY CLOBES MERIWETHER
& SPRENGEL LLP**
150 S. Wacker, Suite 3000
Chicago, Illinois 60606
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com

Jeffrey W. Herrmann, Esq.
**COHN LIFLAND PEARLMAN
HERRMANN & KNOPF LLP**
Park 80 West-Plaza One
250 Pehle Avenue, Suite 401
Saddle Brook, NJ 07663
Telephone: (201) 845-9600
Facsimile: (201) 845-9423
JWH@NJLAWFIRM.COM

Scott Edelsberg, Esq
EDELSBERG LAW, PA
2875 NE 191st Street, Suite 703
Aventura, FL 33180
Telephone: 305-975-3320
scott@edelsberglaw.com

Hassan A. Zavareei
Mark A. Clifford
TYCKO & ZAVAREEI LLP
1828 L Street, NW – Suite 1000
Washington, D.C. 20036
Tel: (510) 254-0900
Fax: (202) 973-0959
hzavareei@tzlegal.com
mclifford@tzlegal.com

Andrew J. Shamis, Esq.
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 1205
Miami, FL 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com

Gary M. Klinger (pro hac vice
forthcoming)
MASON, LIETZ & KLINGER, LLP
227 w. Monroe St., Ste. 2100

Chicago, Illinois 60606
Phone: 847.208.4585
gklinger@masonllp.com

Gary F. Lynch
Jamisen A. Etzel
CARLSON LYNCH LLP
1133 Penn Avenue
Floor 5
Pittsburgh, PA 15222
Telephone: 412-322-9243
Facsimile: 412-231-0246
glynch@carlsonlynch.com
jetzel@carlsonlynch.com

Nick Suciu III, Esq.
BARBAT, MANSOUR & SUCIU PLLC
Barbat Mansour & Suciu PLLC
Bloomfield Hills, Michigan 48302
Tel: (313) 303-3472
nicksuciu@bmslawyers.com

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that, on May 11, 2020 I electronically filed the foregoing with the Clerk of the Court using the ECF system which will notify all counsel of record authorized to receive such filings.

THE MILLER LAW FIRM, P.C.

/s/ E. Powell Miller
E. Powell Miller (P39487)
950 W. University Dr., Ste. 300
Rochester, Michigan 48307
Telephone: (248) 841-2200
epm@millerlawpc.com